Access Professional Edition

Video Verification

BOSCH

en Operation Manual

Table of contents

1	**Overview**	**4**
2	**General**	**5**
2.1	User Login	5
3	**Video Verification**	**8**
3.1	Video verification	9
3.2	Switching video verification on/off	13
4	**UL 294 Requirements**	**14**

1 Overview

The Access Professional Edition System (hereunder referred to as **Access PE)** provides a self-contained access control for small and medium sized companies. It consists of several modules:

- LAC Service: a process which is in constant communication with the LACs (Local Access Controllers – hereafter referred to as Controllers). AMCs (Access Modular Controllers) are used as Controllers.
- Configurator
- Personnel Management
- Logviewer
- Alarm Management
- Video Verification

The modules can be divided into server and client modules.
The LAC service needs to remain in constant contact with the controllers because firstly it constantly receives messages from them regarding movements, presence and absence of cardholders, secondly because it transmits data modifications, e.g. assignment of new cards, to the controllers, but mainly because it carries out meta-level checks (access sequence checks, anti-passback checks, random screening).
The Configurator should also run on the server; however it can be installed on client workstations and operated from there.
The modules Personnel Management and Logviewer belong to the Client component and can be run on the Server in addition, or on a different PC with a network connection to the server.
The following Controllers can be used.

- AMC2 4W (with four Wiegand reader interfaces) - can be extended with an AMC2 4W-EXT
- AMC2 4R4 (with four RS485 reader interfaces)

2 General

2.1 User Login

The following applications are available. The the respective User manuals for details:

Personnel Management

Configurator

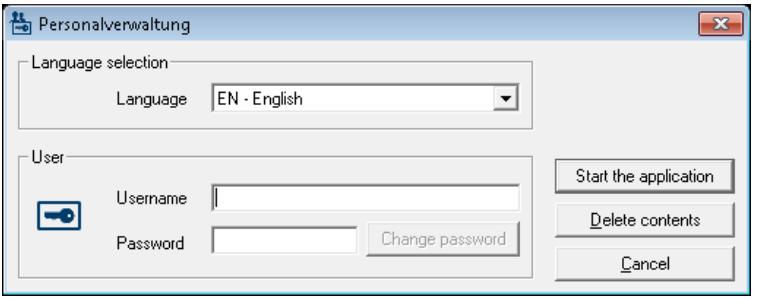
Logviewer

Map and Alarm Management

Video Verification

The system's applications are protected from unauthorized use.
The **default passwords** on first usage are:

- Username: **bosch**
- Password: **bosch**

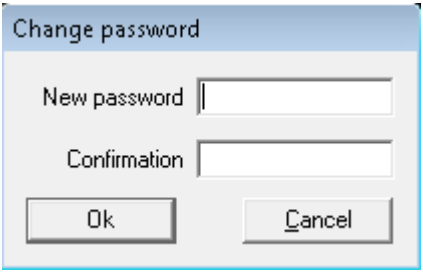


The upper drop-down list can be used to select the desired interaction **language**. The default is that language which was used to install the application. If there is a change of user without restarting the application then the previous language is retained. For this reason it is possible for a dialog box to appear in an undesired language. In order to avoid this, please log in to Access PE again.
Access PE applications can be run in the following languages:

- English
- German
- French
- Japanese
- Russian
- Polish
- Chinese (PRC)
- Dutch
- Spanish
- Portuguese (Brazil)

Notice!
All facilities such as device names, labels, models and user-rights schemes are displayed in the language in which they were entered.Similarly buttons and labels controlled by the operating system may appear in the language of the operating system.

If a valid username/password pair are entered then the button **: Change Password** appears. This can be used to start a new dialog to change the password.



Notice!
Do not forget to change the password!

The button **Start the application** checks the user's privileges and, based on these, starts the application. If the system is unable to authenticate the login then the following error message appears**: Wrong username or password!**

3 Video Verification

You can use video verification to make sure that the person requesting access is actually the card holder; to do this, check the card and authorization data.

Notice!

If video verification is activated for at least one entrance (PE Configurator > Entrances > Select the entrance you want to edit > Video configuration), you must also start the Video verification dialog on at least one workstation; if you do not, **all** access requests will be denied.

When the video system is installed additional facilities are activated in Personnel Management, which serve to make the video system more useful and versatile.

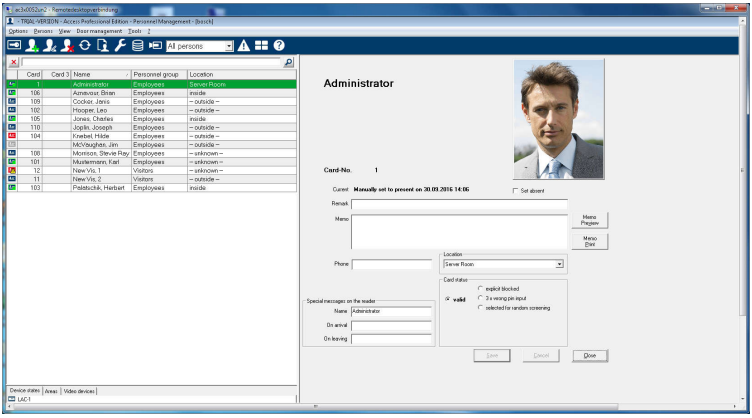
See also

– *Video verification, page 9*

3.1 Video verification

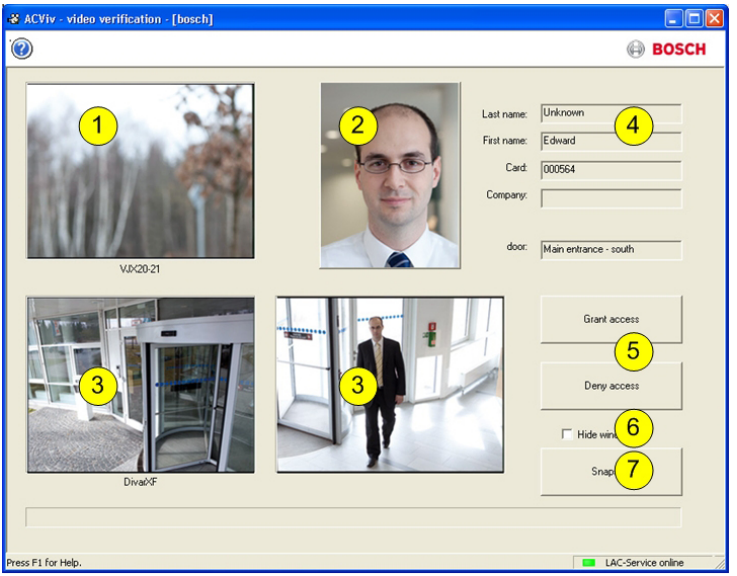
Description of dialogs

Start the application by pressing the  button in Personnel Management.



If there are no current access requests, the dialog displays the default page. If an authorized person scans their card at the entrance, the dialog switches to the views from the relevant cameras.

If the workstation user is currently engaged in other activities, any access requests will bring the Video verification dialog to the foreground.



1 =	**Identification camera** - transmits a live image of the person requesting access.
2 =	**Database image** - an archive image is displayed for comparison with the live image.
3 =	**Surveillance cameras** - the camera showing the back view is shown first, then when the door is unlocked, the display switches to the front view camera.
4 =	**Personnel data** - display showing the data stored in the database for the card number scanned.
5 =	**Grant access/Deny access** - buttons for releasing or locking the door in question.
6 =	**Hide window** - closes the dialog after video verification has been successfully completed and brings it back to the foreground the next time an access request is made.
7 =	**Snapshot** - still images are stored locally from all three camera views.

Requirements

The following facilities are necessary to enable this check, which is carried out by comparing a live image and an archive image.

- Images of the card holder are stored in the database.
- A camera is installed in such a way that it can create a facial view of the person requesting access.
- Up to two cameras recording the area behind the person requesting access — optional.
- Up to two cameras recording the area through the door — optional.
- Door configuration
  - Mark this is as an **Entrance with video verification**.
  - Set video verification to **Active**.
  - Select a device to use as the **Identification camera**.
  - Optional — other cameras to monitor the back or front area.
- At least one permanently manned workstation on which the **Video Verification** application has been installed and started.
  This can run on several workstations at the same time. However, incoming access requests are only sent to one workstation to avoid duplicate or even contradictory processing.

Access procedure for an authorized person

1. Person scans card
   - Card data checked
   - Authorizations checked
2. Video Verification application connected
   If available and configured:
   - Top left: live image from the identification camera
   - To the right of that: archive image of card holder
   - To the right of that: card holder's data — Last name, First name, Card and Company, along with the entrance at which the person is waiting

- Bottom left: live image from the first surveillance camera for the back area
- To the right of that: live image from the second surveillance camera for the back area

3. The workstation user
   - makes sure that the live image matches the archive image and checks the recordings from the surveillance cameras.
   - grants/denies access depending on the outcome of the comparison and checking activities.
4. Video Verification application
   - When the door is unlocked, the bottom two displays from the surveillance cameras switch to the cameras monitoring the front area. This image remains on the screen until the door closes.

Notice!
You can store any number of still images from the camera images displayed locally at any time. Press the **Snapshot** button to save an image from each video.

Dialog activation
After you have started the Video verification dialog, it switches to showing the default. You cannot edit any data or process the dialog when it is in this state. When an **authorized** person requests access at an entrance **configured** and **activated** for video verification, the display shows images from the installed cameras and the corresponding data from the database.
If other applications were being used on the workstation when the request was made, thus pushing the Video verification dialog into the background, the dialog is automatically brought to the foreground at this point.
Once the access request has been processed, the dialog view switches back to the default but remains in the foreground.

If you do not wish to work with this setting, you can select the **Hide window** option to automatically minimize (iconify to the taskbar) the dialog after each verification process; this option also brings the dialog to the foreground each time a new request is received.

3.2 Switching video verification on/off

The context menu of entrances/readers [in the device status list] also offers the function **Deactivate video verification**. This allows, for example, a temporary shortening of the access request process, or conversely, the rapid activation of video verification without the need to change the configuration.
When video verification is switched off, the corresponding entry in the context menu is marked with a tick.
The function is only available for those entrances for which video verification has been activated in the configuration data.
The activation/deactivation of video verification is controlled by the LAC-Service. This distributes the information to all workstations so that the settings can be modified from any of them.

4 UL 294 Requirements

Features not evaluated by UL:

- The Video Verification System
- Map Viewer and Alarm Management with Map and Video Verification
- Video Player
- Log Viewer
- User Rights
- Personnel Management
- Burglar Alarm Use

Features evaluated by UL:

- APE-SW as supplementary monitoring equipment

Bosch Access Systems GmbH
Charlottenburger Allee 50
52068 Aachen
Germany
www.boschsecurity.com